RMT:DKK/JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A BLACK LG SMART CELLULAR PHONE, CURRENTLY IN THE POSSESSION OF THE JOINT TERRORISM TASK FORCE IN BROOKLYN, NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 411

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since July 2018. Since 2019, I have been assigned to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a BLACK LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020, as described in greater detail herein (hereinafter the "Device"). The Device is currently located in the possession of one or more agents from the JTTF in Brooklyn, New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND ON ISIS AND AQAP

6. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224. On or about December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

7. On or about May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224, to add the alias Islamic

State of Iraq and the Levant ("ISIL") as its primary name and to remove all aliases associated with al-Nusrah Front. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS - which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIS FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

8. On January 19, 2010, the Secretary of State designated al-Qa'ida in the Arabian Peninsula (AQAP), also known as al-Qa'ida of Jihad Organization in the Arabian Peninsula, also known as Tanzim Qa'idat al-Jihad fi Jazirat al-Arab, also known as al-Qa'ida Organization in the Arabian Peninsula (AQAP), also known as al-Qa'ida in Yemen (AQY), also known as al-Qa'ida in the South Arabian Peninsula, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224. To date, AQAP remains a designated FTO.

PROBABLE CAUSE

9. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder),[1] 18 U.S.C. § 922(g)(5) (possession of a

[1] Section 231(a)(3) provides, in relevant part: "(3)Whoever commits or attempts to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely

firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization).

10. In or about late May 2020 and early June 2020, a series of demonstrations and protests occurred in New York City. These actions included the gathering of large crowds in Brooklyn, New York, including at night. Although the vast majority of individuals participating in these demonstrations have acted peacefully, a minority of individuals have engaged in looting, violence against law enforcement officers and other criminal conduct while the demonstrations were ongoing.

11. As a result of the demonstrations, hundreds of NYPD officers were deployed throughout New York City, including in Brooklyn. In addition, as a result of the civil unrest, on June 2, 2020, New York State Governor Andrew Cuomo and New York City Mayor Bill de Blasio announced a citywide curfew. NYPD officers helped to enforce the curfew. On June 3, 2020, a citywide curfew was in effect beginning at 8:00 p.m.

12. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. The two officers were assigned to an anti-looting post that evening, including the responsibility for enforcing the curfew. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching

---

affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function—Shall be fined under this title or imprisoned not more than five years, or both."

the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer in a clear attempt to kill him. CAMOVIC then ran back toward the first officer, whom he had already stabbed, and attempted to stab him again. A struggle ensued. Video footage from the officer's bodycam shows that CAMOVIC fought for control of the officer's service weapon and ultimately gained control of it and fired multiple shots at several officers, including at one or more officers who responded to the scene.

13. CAMOVIC was ultimately shot by responding officers and taken in to custody.

14. A review of bodycam footage revealed that at multiple points during his attack on the NYPD officers, CAMOVIC yelled "Allahu Akbar." Based on my knowledge, training and experience, I know that Allahu Akbar is an Arabic phrase that means "God is the greatest" and is frequently exclaimed by perpetrators of violent jihadist attacks during such attacks.

15. On or about June 4, 2020, CAMOVIC's father provided consent to law enforcement officers to search his apartment, where CAMOVIC also resides. During a search of CAMOVIC's bedroom, which CAMOVIC's father has regular access to, officers discovered DVDs indicating that they contained violent jihadist propaganda. Specifically, officers observed multiple compact discs or DVDs marked "Abu Bakr," a possible reference to Abu Bakr al-Baghdadi, the now deceased self-proclaimed leader of the Islamic State in Iraq

and Syria ("ISIS"), a foreign terrorist organization that, since 2013, has claimed credit for numerous terrorist activities, including the November 2015 terrorist attacks in Paris, France, and the March 2016 suicide bombings in Brussels, Belgium, among many others. Officers also observed in CAMOVIC's room multiple compact discs or DVDs marked "Anwar al-Awlaki," including one that also included the word "jihad." Al-Awlaki was a United States-born radical Islamic cleric and prominent leader of the foreign terrorist organization al Qaeda in the Arabian Peninsula who was killed on or about September 30, 2011. Even now, nearly nine years after his death, al-Awlaki is still commonly regarded as the leading figure inciting English-speaking Muslims to participate in violent jihad.

16. Based on my knowledge, training and experience, the confident, aggressive and unprovoked nature of the attack, including his text message to Individual 1 immediately before the attack that he would "be a while" and the fact that he was already holding the knife which he immediately used to attack the officers, indicates that his attack on the officers was planned and premediated.

17. Law enforcement officers searched CAMOVIC's person incident to his arrest, during which time they recovered the Device.

18. Phone records and interviews of CAMOVIC's associates reflect that his cell phone number is 347-394-9934, which is the phone number for the Device.

19. The investigation has revealed that earlier on June 3, 2020, hours before his attack, CAMOVIC had dinner with two associates in Brooklyn (hereinafter "Individual 1" and "Individual 2") and that, after dinner, the three individuals separated. Toll records for the

Device as well as text messages and additional information provided to law enforcement by Individual 1 indicate that CAMOVIC exchanged messages with Individual 1 about possibly meeting again on the evening of June 3. At approximately 11:09 p.m., CAMOVIC texted Individual 1 asking about Individual 1's whereabouts. Individual 1 responded that he would be home soon and then wrote, "Wut up. Btw that shooting that u said, [Individual 2] called me B4 and said that cops came to him for cameras. Some guy killed to ppl."[2] CAMOVIC responded "damb" and then informed Individual 1 that he was on Ocean Avenue, near Individual 1's home. Individual 1 then responded "U waiting for me? Imma be there in like 5." CAMOVIC responded "kk" and then, at 11:38 p.m.—approximately 12 minutes before his attack on police—CAMOVIC wrote, "Ill be a while."

20. Based on a comparison of the toll records for the Device and the screenshots of text messages that Individual 1 provided to law enforcement, it appears that Individual 1 may have sent to the Device one additional text message at approximately 11:10 p.m. which was not captured in the screenshots Individual 1 provided to law enforcement. The toll records indicate that the apparently missing text message was sent by Individual 1 to CAMOVIC seconds before or seconds after Individual 1's text message to CAMOVIC that police had questioned Individual 2 about a shooting ("Btw that shooting that u said, [Individual 2] called me B4 and said that cops came to him for cameras. Some guy killed to ppl.").

---

[2] Law enforcement officers are attempting to identify the shooting incident that Individual 1 referred to in his June 3, 2020 text message to CAMOVIC.

21. Toll records for the Device further show that, in addition to his communications with Individual 1 immediately before the attack, CAMOVIC also used the Device to exchange multiple text messages with another other individual ("Individual 3") in the hours before the attack. Specifically, toll records for the Device show that CAMOVIC used the device to exchange approximately five text messages with Individual 3 between approximately 7:00 and 10:00 p.m. on June 3, 2020.

22. Immigration records associated with CAMOVIC's father show that CAMOVIC was born outside of the United States and has no legal immigration status in the United States. Accordingly, CAMOVIC likely violated 18 U.S.C. § 922(g)(5), which prohibits illegal aliens from possessing firearms, in attempting to take control of and firing an NYPD officer's service weapon.

23. Based on my training and experience, I know that individuals who plan attacks on law enforcement often use cellular phones to do so, including by communicating with others regarding their attack plans, researching and locating targets, planning their route of attack and/or escape, searching for weapons and posting content on social media regarding their mental state and intentions. There is also probable cause to believe that, because CAMOVIC was carrying the Device on his person at the time of the attack, the Device will contain evidence of his location immediately prior to the attack and possibly whether and where he met with any coconspirators before the attack. Furthermore, there is probable cause to believe that the text messages stored on the Device will resolve the apparent discrepancy between the toll records for the Device and the screenshots of text messages provided to law enforcement

by Individual 1. As noted above, these texts appear to relate to a shooting and to statements made to law enforcement officers investigating said shooting.

24. Based on the foregoing, I submit that this affidavit establishes probable cause to search the Device. Your affiant is further requesting to share the information obtained from this search warrant (to include copies of digital media and social media applications) with any government agency investigating, or aiding in the investigation, or this case or related matters.

25. The Device is currently in the possession of the JTTF in Brooklyn, New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the JTTF.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless

telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing

computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation as not all of the subjects and targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Colin J. McLafferty

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 4, 2020:

Steven M. Gold

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a BLACK LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020, as described in greater detail herein (hereinafter the "Device"). The Device is currently located in the possession of the Joint Terrorism Task Force in Brooklyn New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Device, described in Attachment A, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, committed between May 25, 2020 and the present, including:

1. All records and information on the Device including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

6. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

7. Location information for the Device from 12:00 p.m. on June 3, 2020 to 12:00 a.m. on June 4, 2020.

8. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.